Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232

COMMENTS OF DAHUA TECHNOLOGY USA INC.

Andrew D. Lipman
Russell M. Blau
Patricia Cave

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
patricia.cave@morganlewis.com

Counsel to Dahua Technology USA Inc.

September 20, 2021

EXECUTIVE SUMMARY

The rules proposed in this proceeding to ban all equipment on the Covered List from obtaining equipment authorizations exceed the Commission's authority under the Communications Act, the Secure and Trusted Communications Networks Act (the "Secure Networks Act") and also are outside of the Commission's ancillary jurisdiction. The Commission's equipment authorization rules seek to address harmful interference of RF equipment, not national security, and the Secure Networks Act applies only where Federal funds are used directly or indirectly to acquire covered equipment or services.

The proposed rules also are arbitrary and capricious because they seek to ban equipment from the U.S. market based solely on the identity of the manufacturer rather than any technical considerations relevant to protection against RF interference and other technical threats. Moreover, there is no rational reason to treat all equipment on the Covered List as a threat to national security based solely on the identity of the manufacturer rather than any technical parameters of a particular item. Nor is there any evidence that Dahua's equipment causes excessive RF interference or fails to meet any other technical standard considered in the equipment authorization process. The proposed rules therefore are unlawful and must be rejected. While the proposed rules should be abandoned because they exceed the Commission's authority and are arbitrary and capricious, the Commission must (at a minimum) make clear that the rules are not a categorical ban on all Dahua equipment and that equipment produced or provided by Dahua that is not used for the purposes delineated in Dahua's entry on the Covered List remain eligible for authorization.

The proposed rules also violate Dahua's constitutional rights. If adopted, the proposed rules would be unconstitutionally retroactive to the extent they seek to permit revocation of existing authorizations based on non-technical criteria and qualifications that did not exist at the time the

authorizations were granted. And, because equipment authorizations are protected property rights, any and all revocations must be conducted (if at all) with regard to the holder's constitutional rights to due process (including the opportunity for notice and a hearing).

Finally, the costs of the proposed rules as applied to Dahua vastly exceed any speculative benefits that may derive from their imposition. The rules could require the removal and replacement of millions of devices (many of which are not connected to public communications networks) by users large and small across a wide array of industry sectors. Moreover, banning equipment from leading manufacturers in the video security segment will limit the supply of such equipment, necessarily driving up the prices paid by U.S. end-users for equipment from other suppliers.

Putting the costs of implementation to the side, it is questionable as to whether enforcement of the proposed rules would be practicable particularly as concerns Dahua's equipment, given the prevalence of white-label products in the industry. The Commission (and others) also will be limited in their ability to enforce the rules due to the lack of visibility or connection to end-user customers that are not telecommunications carriers.

For all of these reasons, the Commission should abandon this proceeding and should not adopt its proposed rules.

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232

COMMENTS OF DAHUA TECHNOLOGY USA INC.

Dahua Technology USA Inc. ("Dahua USA"), by its undersigned counsel, submits these comments regarding the Notice of Proposed Rulemaking ("NPRM") in the above-captioned docket.[1] For the reasons described below, the Commission should abandon this proceeding and should not adopt its proposed rules.

I. INTRODUCTION

A. About Dahua Technology USA

Dahua USA is a wholly owned subsidiary of Zhejiang Dahua Technology Co., Ltd. ("Dahua Technology", and together with Dahua USA and its affiliates, "Dahua"). Dahua Technology, founded in 2001, is a publicly traded company on the Shenzhen Stock Exchange with a diversified shareholder base. Only a miniscule portion of Dahua Technology's ownership (via shares held on the Shenzhen Stock Exchange) is indirectly (through state-owned enterprises) attributable to the government of the People's Republic of China or other government entities. Such entities are not

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, et al.*, Notice of Proposed Rulemaking, ET Docket No. 21-232, EA Docket No. 21-233, FCC 21-73 (rel. Jun. 17, 2021) ("*NPRM*").

represented on its board of directors or in its management. In practice, Dahua Technology is a private sector business that is not controlled or operated by any government.

Dahua is an industry-leading video-centric smart Internet of Things ("IoT") solutions and service provider that delivers high value, reliable performance, and excellent technical support. Dahua USA, the U.S. affiliate, was formed in 2014 and currently is headquartered in Irvine, California. In the United States, Dahua USA directly employs approximately 85 U.S.-based employees in 18 states and indirectly (through suppliers) is responsible for additional U.S.-based employment in areas including logistics and warehousing. Dahua USA's primary business operations includes sales, technical support, warehouse, operations, marketing and providing local product teams to support market needs in North America. Together with its affiliates, Dahua USA offers end-to-end security solutions, systems, and services to add value for city operations, corporate management, and consumers. Although many of Dahua USA's products are video security (or, in limited cases, telecommunications) equipment, Dahua USA offers a range of other products that are not, such as cables, displays, power supplies, alarm sensors, storage devices, intercoms, and access control solutions, among others. Dahua's products imported to, marketed, and sold in the United States have been certified through the Supplier's Declaration of Conformity ("SDoC") procedures by FCC-authorized labs or through the Commission's certification procedures, to the extent applicable.

In the United States, Dahua USA conducts business through two primary business divisions. Through its Original Equipment Manufacturer ("OEM") Division, Dahua USA sells products that other vendors rebrand as their own for resale to end-user/retail customers (directly or indirectly through distributors and retailers). These products are sold by U.S. vendors, distributors, and retailers to customers of all types and sizes. Currently, Dahua works with approximately 50

OEM customers in the United States, with 34 OEM partners having placed an order with Dahua in the last 12 months. Through its Branded Division, Dahua USA focuses on direct and indirect sales of products under the "Dahua" brand to small and mid-sized businesses ("SMBs") as well as sales of related vertical solutions. These products are offered to a wide range of industry customers. Currently, Dahua USA cooperates directly with approximately 137 distributors, with more than 8,000 registered dealers in the United States. A substantial portion of Dahua USA's top registered dealers in the U.S. are small businesses. In addition to direct and indirect product sales, Dahua USA provides technical support, product training, after-sales services, and marketing support to all its customers.

Dahua is focused on adopting privacy and cybersecurity practices to protect its customers. For example, Dahua established a dedicated "Network Security and Data Protection Special Team" that is responsible for real-time tracking and interpretation of global privacy compliance dynamics. Dahua's privacy practices are certified according to ISO/IC 27701:2019 standards and its products are certified as compliant with ETSI TS 103645 standards. Dahua also established the Dahua Cybersecurity Center ("DHCC") to address cybersecurity issues and provide more robust and secure products and solutions for Dahua's global customers.[2] The DHCC consists of security vulnerability reporting (including notices and announcements of vulnerabilities) and cybersecurity knowledge sharing with Dahua's global customer base.[3] The Product Security Incident Response Team ("PSIRT"), an integral part of the DHCC, is responsible for receiving, processing, and disclosing Dahua product and solution-related security vulnerabilities. Dahua encourages its end-user

---

[2] *See* Dahua Cybersecurity Center (DHCC), https://www.dahuasecurity.com/support/cybersecurity.

[3] For additional information regarding Dahua's approach to cybersecurity, please see: https://us.dahuasecurity.com/?page_id=50564.

customers, partners, suppliers, government agencies, industry associations, and independent researchers to report potential risks or vulnerabilities to PSIRT by email. To Dahua's knowledge, there has never been an example (in the United States or elsewhere) of Dahua's equipment being used for espionage or untoward purposes. Any such concerns are purely speculative.

B. The Commission Should Not Adopt its Proposed Rules

As explained further below, the proposed rules exceed the Commission's authority under the Communications Act and should not be adopted. No provision of the Communications Act gives the Commission authority to prohibit authorization of equipment based solely on the identity of the manufacturer. As a result, they are unlawful and must be rejected.

Moreover, the proposed rules are arbitrary and capricious, lacking any rational relationship to the purpose of the equipment authorization rules. If adopted, the proposed rules would preclude authorization of equipment without any connection to conformity with technical standards that underpin the authorization rules and the Commission's authority in this area. As with rules that exceed the Commission's authority prescribed by Congress, arbitrary and capricious rules are unlawful and must be rejected.

The proposed rules also raise constitutional concerns that counsel against their adoption. First, the proposed framework to prohibit equipment authorizations based solely on the identity of the manufacturer would constitute an unlawful bill of attainder in violation of the U.S. Constitution. Second, the proposed rules will be unlawfully retroactive as applied. Third, the proposed rules providing for revocation of existing authorizations violate Dahua's constitutionally protected property rights.

Finally, the proposed rules should be rejected because their costs will exceed any speculative benefits generated from their implementation and enforcement. The proposed rules would have significant unintended and disproportionate impacts on U.S. users and entities, including

OEMs, distributors, integrators, installers, and end-user customers. Dahua USA's equipment provides significant value to the U.S. marketplace, including for education, agriculture and other users in the U.S. Without the ability to repair, replace or purchase new equipment, individuals and entities in the U.S. will face significant difficulty and increased costs (including for potentially required removal and replacement of equipment already in use). Limiting Dahua USA's access to the U.S. market through a ban on future authorizations for RF-emitting equipment, and potential revocation of existing authorizations for equipment already deployed, would result in direct and indirect job loss and other harms to the U.S. economy. Moreover, limiting Dahua USA's access to the U.S. market would result in less competition in the U.S. security industry and higher prices for security products. Finally, the proposed rules face significant enforcement barriers such that enforcement would be unreasonably expensive at best, and infeasible at worst, rendering any potential benefits of the rules illusory.

II. THE PROPOSED RULES EXCEED THE COMMISSION'S AUTHORITY AND ARE UNLAWFUL.

The NPRM includes several proposals, each of which lacks any foundation in the Commission's authority (ancillary or otherwise) pursuant to the Communications Act. First, the Commission proposes to ban from authorization all equipment included on the Covered List adopted pursuant to the Secure and Trusted Communications Networks Act ("Secure Networks Act"), whether through the certification process or the SDoC procedures.[4] Second, the Commission proposes to require any and all equipment from Covered List suppliers to obtain authorization through

[4] *See* NPRM, App. A (proposed § 2.903). The NPRM also proposes to exclude Covered List equipment from exemptions to the equipment authorization rules. *See* NPRM, ¶ 76.

the certification process[5] and exclude these suppliers from using the SDoC process.[6] Finally, the Commission seeks comment on the extent to which it should revoke existing equipment authorizations granted pursuant to processes and procedures in place before adoption of final rules in this proceeding, and the specific procedures the Commission should use if and when it seeks to revoke an existing equipment authorization.[7] These proposed rules exceed both the Commission's express authority under the Communications Act and Secure Networks Act and also are outside of the Commission's ancillary jurisdiction.

A. No Provision of the Communications Act Authorizes Withholding or Revoking Equipment Authorizations Based on National Security Considerations.

The Communications Act does not authorize the Commission to adopt the proposed rules. The Commission's equipment authorization rules were adopted pursuant to Section 302 of the Communications Act.[8] Section 302 empowers the Commission to "make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio

5 *See* NPRM, App. A (proposed § 2.907).

6 *See* NPRM, App. A (proposed § 2.906).

7 *See* NPRM, ¶¶ 82-89.

8 47 U.S.C. § 302a.

frequency energy." However, the proposed rules have no regard for or connection with radio interference concerns, the plain focus of Section 302. Rather, the sole purpose of the proposed rules is to prohibit equipment authorizations simply because an entity is named on the Covered List.[9]

The NPRM notes that the equipment authorization rules are not addressed exclusively to interference concerns. The Commission has amended the rules over the years to "address other policy objectives – such as human RF exposure limits, hearing aid compatibility with mobile handsets, and the Anti-Drug Abuse Act of 1988",[10] but each of those "other policy objectives" is tied specifically to a statute that gave the Commission express authority and/or imposed an obligation for the Commission to adopt and enforce additional requirements. For example, the National Environmental Policy Act ("NEPA") requires the Commission "to evaluate the effects of its actions on the quality of the human environment, including human exposure to RF energy emitted by Commission-regulated transmitters and facilities."[11] Likewise, Section 710 of the Communications Act requires the Commission to "establish such regulations as are necessary to ensure reasonable access to telephone service by persons with impaired hearing"[12] and to adopt specific requirements for customer premises equipment to be hearing aid compatible.[13] Similarly, the Anti-

---

9 *See* NPRM, ¶ 76 (seeking comment "on whether the Commission should consider possible revisions or clarifications to the Commission's rules to address issues related to 'covered' equipment and the potential of such equipment, *regardless of RF emissions characteristics*, to pose an unacceptable risk to U.S. networks or users") (emphasis added).

10 NPRM, ¶ 23.

11 *See Proposed Changes in the Commission's Rules Regarding Human Exposure to Radiofrequency Electromagnetic Fields, et al.*, Resolution of Notice of Inquiry, Second Report and Order, Notice of Proposed Rulemaking, and Memorandum Opinion and Order, 34 FCC Rcd 11687, 11688, ¶ 1 (2019).

12 *See* 47 U.S.C. § 610(a).

13 *See* 47 U.S.C. § 610(b).

Drug Abuse Act of 1988 imposes specific limitations on the federal benefits for individuals convicted of federal offenses related to trafficking in or possession of controlled substances.[14] Thus, although the equipment authorization rules go beyond simply implementing Section 302, each of their requirements is derived from some express statutory grant of regulatory authority.

In contrast, there is no statute that explicitly gives the Commission any authority, responsibility, or direction to withhold (or revoke) equipment authorizations based on national security considerations. Section 302 is limited to regulation of equipment in the context of "the interference potential of devices that emit [RF] energy and that can cause harmful interference to radio communications."[15] Section 302 states that "[t]he Commission may, consistent with the public interest, convenience and necessity, make reasonable regulations (1) governing the interference potential of devices … and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[16] Therefore, the "public interest" analysis under this section must be focused specifically on the interference potential and susceptibility to interference of devices, neither of which has any connection to the identity of a manufacturer.

---

14 *See* 21 U.S.C. § 862.

15 NPRM, ¶ 23. *See also* H. Rep. 90-1108, at 8 (1968) ("The chief purpose of this legislation is to give the Commission adequate authority to deal with increasingly acute interference problems arising from expanded usage of electrical and electronic devices which cause, or are capable of causing, harmful interference to radio reception.").

16 47 U.S.C. § 302a(a).

B. The Proposed Rules Exceed the Commission's Ancillary Jurisdiction.

Nor are the proposed rules within the Commission's ancillary jurisdiction under Section 4(i) of the Communications Act.[17] "The FCC's ancillary jurisdiction may be broad, but it is not unbounded."[18] Although the NPRM argues that the proposed rules would be "reasonably necessary to the effective enforcement of the Secure Networks Act,"[19] case law holds that the Commission may exercise ancillary jurisdiction in situations not explicitly addressed in the Communications Act *only* when (a) the matter is within the general scope of the agency's jurisdiction or expertise under Title I of the Communications Act and (b) the proposed regulation is reasonably ancillary to enforcement of some specific statutory provision (*i.e.*, to one of the Commission's statutorily mandated responsibilities).[20] Therefore, the Commission has only limited authority to exercise jurisdiction over matters not expressly addressed by the Communications Act. Although the Commission has general authority to regulate RF-emitting equipment pursuant to the Communications Act, the second prong of the ancillary jurisdiction test is not met in this case.

The Secure Networks Act is very specific and does not leave the Commission the kind of discretion that supports a finding of ancillary jurisdiction. The Secure Networks Act restricts dis-

---

17 *See* 47 U.S.C. § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.").

18 *EchoStar Satellite L.L.C. v. FCC*, 704 F.3d 992, 999 (D.C. Cir. 2013).

19 NPRM, ¶ 69. *See also* NPRM, ¶ 65 (stating that "in order to ensure that the Commission's rules under the Secure Networks Act effectively preclude use of equipment on the Covered List by USF recipients as contemplated by Congress, it is necessary to rely on the Commission's established equipment authorization procedures to restrict further equipment authorization, and the importation and marketing, of such devices in the first instance").

20 *See Comcast Corp. v. FCC*, 600 F.3d 642, 645 (D.C. Cir. 2010) (citing *Am. Library Ass'n v. FCC*, 406 F.3d 689, 691-92 (D.C. Cir. 2005)).

tribution of Commission-administered subsidy funds and establishes a program to reimburse providers of advanced communications services for the removal, replacement and destruction of certain equipment.[21] Congress clearly intended the Secure Networks Act to apply only where Federal funds were being used directly or indirectly to acquire covered equipment or services; if it had wanted to extend a prohibition beyond that, it would have said so. It did not give the Commission any new authority to take any action restricting "covered" equipment or services other than those specific restrictions mandated by the statute.

The Commission cannot use ancillary jurisdiction to act beyond the specific intent of Congress. For example, a law banning advertising of tobacco products on broadcast television would not give the Commission ancillary jurisdiction to outlaw *all* television advertising (even though such a ban would incidentally serve the purpose of preventing tobacco ads). Similarly, here, a law restricting use of Federal funds to purchase certain equipment cannot empower the Commission to prohibit import, marketing and use of that equipment entirely. The Secure Networks Act does not address (or demonstrate any intent to address) use of the Commission's equipment authorization procedures, and equipment authorization is unrelated to the purpose of the Secure Networks Act.

In any event, the Secure Networks Act establishes an enforcement process that is calibrated to the discrete purposes of that Act. For example, Section 5 establishes a reporting requirement

---

[21] Notably, following Congressional direction, the Commission has limited reimbursement only to equipment on the Covered List that is provided or produced by Huawei or ZTE. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, FCC 21-86, WC Docket No. 18-89, ¶ 18 (rel. Jul. 14, 2021) (determining that "[o]nly equipment and services on the Covered List that are also defined in the 2019 Supply Chain Order or that are produced or provided by covered companies designated under section 54.9 of the Commission's rules as posing a national security threat to the integrity of communications networks or the communications supply chain are eligible for reimbursement under the Reimbursement Program").

whereby providers of advanced communications service (*i.e.*, the entities most likely to receive Commission-administered subsidy funds) must report whether the provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service.[22] Further, Section 7 outlines the penalties for violations of the Act.[23] Therefore, it is unnecessary (and duplicative as applied to advanced communications service providers that use telecommunications equipment) for the Commission to take additional action in this proceeding that would not accomplish the Secure Networks Act goals of restricting use of Commission-administered subsidy and Reimbursement Program funding.

Nor can the Commission rely on other provisions it cites as providing ancillary authority to adopt the proposed rules. Although the Commission cites to its authority to prescribe "the nature of service to be rendered by radio licensees under section 303(b) of th[e] Act[,]"[24] that provision applies in the context of "class[es] of licensed station and each station within any class" and does not apply generally to *non-licensed* users of equipment that has been (or will be) authorized through the Commission's equipment authorization process. Nor does the Commission's equipment authorization process and obtaining equipment authorization have any practical or other connection to the *type of service* to be rendered through the equipment so authorized. This provision therefore is irrelevant to the proceeding and does not provide any specific authority to which the Commission can tether an assertion of ancillary jurisdiction.

---

22 *See* 47 U.S.C. § 1604(a).

23 *See* 47 U.S.C. § 1606.

24 NPRM, ¶ 69.

Moreover, although Section 303(e) of the Communications Act mentions "external effects" of equipment,[25] its context makes clear that this phrase only refers to equipment used by licensed operators of radio transmitters and the effects of such transmissions, including the purity and sharpness of the RF emissions from apparatus in each radio station. It does not, as the Commission implies, grant authority (ancillary or otherwise) for the Commission to prevent importing, marketing or sale of equipment based solely on the identity of the supplier (which has nothing to do with the "effects" of equipment).[26]

Nor does Section 303(g) provide any authority for the Commission to ban equipment produced or provided by named manufacturers from the equipment authorization process.[27] When read in full context, Section 303(g) addresses the study of "new uses for radio", "experimental uses of frequencies", and "generally encourage[ing] the larger and more effective use of radio in the public interest[.]"[28] Similarly to Sections 302 and 303(e), this provision has nothing to do with the identity of the manufacturer of RF-emitting equipment or national security risks that such equipment may or may not pose.

Finally, the Commission does not have jurisdiction (ancillary or otherwise) to impose restrictions on equipment authorizations for named companies due to the authorities granted by the Communications Assistance for Law Enforcement Act ("CALEA"). CALEA does not address equipment authorization, nor use of non-telecommunications equipment by non-carriers. Nor does

---

25 *See* 47 U.S.C. § 303(e) (requiring the Commission to "from time to time … [r]egulate the kind of apparatus to be used with respect to its external effects and the purity and sharpness of the emissions from each station and from the apparatus therein").

26 *See* NPRM, ¶ 66.

27 *See* NPRM, ¶ 65 (citing to Section 303(g) for the proposition that the Commission "relies on the equipment authorization process to implement other statutory duties, including the duty to promote efficient use of the radio spectrum").

28 47 U.S.C. § 303(g).

it provide the Commission with authority to ban wide categories of equipment, in particular non-telecommunications equipment used by the general population.

Like the Secure Networks Act, CALEA has a specific purpose. It only allows the Commission to regulate certain capabilities of equipment used by telecommunications carriers relating to surveillance and interception of communications and to establish limits as to when such capabilities can be activated.[29] Each provision of CALEA also is clearly circumscribed. For example, the plain text of Section 1002(a) establishing capability requirements applies to *telecommunications carriers* and "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications[.]"[30] Section 1002(b)(2) further limits CALEA's application by excluding information services and equipment, facilities or services that only support private networks or interconnection of telecommunications carriers.[31] The provisions therefore apply to particular parties and for equipment used for particular purposes. Likewise, Section 1004 applies only to *telecommunications carriers* and only *within carriers' switching premises*.[32] CALEA, therefore, cannot support prohibiting authorization of video security equipment that is not used by telecommunications carriers; is not located within a carrier's switching premises; does not have the ability to originate, terminate, or direct communications; and lacks any "switching" functionalities whatsoever.

Moreover, CALEA prohibits any law enforcement agency from compelling or preventing "the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic

---

29 *See* 47 U.S.C. §§ 1001-1010.

30 47 U.S.C. § 1002(a)

31 47 U.S.C. § 1002(b)(2).

32 47 U.S.C. § 1004.

communication service."[33] If law enforcement cannot compel or prevent adoption of any specific equipment, it follows that the Commission cannot do the same, in particular where the equipment (a) is not communications equipment in the first instance and/or (b) is not used by providers of wire or electronic communication services. Interpreting CALEA to provide authority for the Commission to prohibit equipment authorizations would be an arbitrary and capricious interpretation of the statute contrary to its purposes to prevent unauthorized interception by law enforcement.[34]

III. THE PROPOSED RULES ARE ARBITRARY AND CAPRICIOUS.

Even when acting within its statutorily defined authorities, the Commission cannot impose rules that are arbitrary and capricious. Any arbitrary and capricious rules are unlawful and must be rejected.[35] The decision to ban equipment from the U.S. market by prohibiting authorization based solely on the identity of its manufacturer, rather than any technical considerations, is arbitrary and capricious, and would be unlawful as a result.

A rule that focuses on the producer rather than technical considerations of particular items of equipment is not rationally related to the purpose of the equipment authorization rules which seek to protect against radio frequency interference and other *technical* threats. In contrast to the rules that prohibit a person with a drug conviction from obtaining equipment authorization,[36] there

---

33 47 U.S.C. § 1002(b)(1).

34 *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Report and Order, 14 FCC Rcd. 4151, 4158, ¶ 20 (1999).

35 *See* 5 U.S.C. § 706(2)(a) (providing that agency actions are unlawful and shall be set assign if found to be "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law"). *See also Judulang* v. *Holder*, 565 U.S. 42, 55 (2011) (stating that even when an agency pursues a "legitimate" goal, it must pursue that goal "in some rational way" that reflects "non-arbitrary, relevant factors").

36 *See* 47 CFR § 2.911(d)(2) (requiring a certification that the applicant is not subject to a denial of Federal Benefits pursuant to the Anti-Drug Abuse Act of 1988).

is no law that mandates banning equipment based on the identity of a manufacturer or provider of the equipment.

Nor is there any rational reason for treating *all* equipment on the Covered List, without regard to the technical parameters of any particular item, as a threat to the public interest and national security. Under the proposed rule, even if a company named on the Covered List could prove with scientific and/or technical certainty that a particular item complied with all applicable technical requirements and posed no potential harm of any kind, it still would not be permitted to obtain an authorization for that item. And, the proposed rule targets even equipment that is not connected to *any* communications network, based solely on the identity of the manufacturer. There is no logical nexus between the Covered List and the equipment authorization process.

The proposed rule would be further arbitrary and capricious as applied to Dahua in particular. There is no evidence that Dahua's equipment causes any excessive RF interference (harmful or otherwise) or fails to meet any other technical standards relevant to the equipment authorization process. And, the Commission has not made any particularized finding that Dahua as a company, or any of the equipment that it manufactures, poses a threat to U.S. national security.[37] Without any statutory authority or rational basis to do so, the Commission should not preclude Dahua from using the equipment authorization process (including any exemptions or the SDoC process).

In any event, however, the Commission should not altogether preclude Dahua from equipment authorization for any equipment that can be used for purposes other than those outlined in its listing in the Covered List, as that listing is derived from Section 889 of the National Defense

[37] *Cf.* 47 CFR § 54.9(b) (establishing a process for designating companies as posing a national security risk to communications networks and communications supply chains).

Authorization Act of 2019 ("Section 889"). Section 889 includes equipment only video surveillance and telecommunications equipment from Dahua used "*for the purpose of* public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes[.]"[38] And, by its terms, the Covered List (as adopted by the Commission) applies to Dahua only "to the extent" Dahua's equipment is used for the specific purposes identified in Section 889.[39] Any restriction on Dahua's use of the equipment authorization process therefore must be tethered to the confines of Section 889 and Dahua's entry on the Covered List. It follows that any equipment produced or provided by Dahua may be eligible for authorization under the Commission's procedures so long as the equipment is not used for one of the purposes delineated in Dahua's entry on the Covered List.

Although the NPRM acknowledges the "use" limitation to Dahua's listing on the Covered List,[40] the Commission does not have authority or expertise to assess the purpose for which equipment may or may not be used as part of the equipment authorization process. Nor do Telecommunication Certification Bodies ("TCBs") have any ability to know in advance, while reviewing Dahua products, who will use Dahua's equipment and/or for what purpose or purposes. TCBs also lack expertise to determine whether the purposes for which Dahua equipment may be used fit the proscribed uses in Dahua's Covered List entry. Beyond challenges in anticipating possible uses for Dahua's equipment, it is unclear who (if anyone) will or practicably can monitor equipment

---

38 *See* Pub. L. 115-232, 132 Stat. 1636, § 889(f)(3)(B) (emphasis added).

39 *See Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice, DA 21-309, at 3 (PSHSB Mar. 12, 2021).

40 NPRM, n.163 (acknowledging the use limitation and implying that the "PSHSB has important regulatory responsibilities and subject matter expertise" to evaluate prospective uses).

after it is sold to determine how the equipment is actually being used by end-users. Further compounding this challenge is that equipment sold directly to an end-user by a manufacturer, or indirectly by a distributor or retailer, may be further resold any number of times such that the original end-user may not be the user for the lifetime of the equipment and the use of the product may change over time. There is no process in place (or that could be efficiently developed) to track all users (or potential users) and uses of equipment to determine whether the uses are permitted or not. It is therefore difficult to conceive of a scenario in which the Commission can practicably implement its proposed rules or how TCBs, as partners with the Commission in the equipment authorization process, can ensure they comply without implementing the rules in an overly prescriptive way.

While Dahua opposes the proposed rules altogether as exceeding the Commission's authority, any guidance issued by the Commission (or its Bureaus or Offices) to industry and other participants in the equipment authorization process must make clear that the rules are not a categorical ban on all Dahua equipment and that equipment produced or provided by Dahua that meets the "use" limitation criteria shall still be eligible for authorization.

IV. THE PROPOSED RULES VIOLATE DAHUA'S CONSTITUTIONAL RIGHTS.

The proposed rules also would violate Dahua's constitutional rights in several ways and therefore should be rejected.

Bill of attainder. The rules, if adopted, would constitute an unlawful bill of attainder. The Bill of Attainder Clause of the U.S. Constitution provides that "No Bill of attainder … shall be passed."[41] "A bill of attainder is a legislative act which inflicts punishment without a [hearing]."[42]

---

41 U.S. Const. art. I, § 9, cl. 3.

42 *United States* v. *Lovett*, 328 U.S. 303, 315 (1946).

A rule that labels a company (or companies) as threats to national security and barring them from importing, marketing and selling their products to any customers imposes a "punishment" without a hearing.[43] The proposed rules would (without any opportunity for a hearing) prohibit the importation, marketing, and use of, and the ability for named companies to obtain authorization for, equipment in the United States based solely on the identity of the manufacturer.

Unreasonable secondary retroactivity. The proposed rules would be unconstitutionally retroactive as applied. It is well established that the Administrative Procedure Act ("APA") prohibits rules that have unreasonable secondary retroactivity. In other words, rules that unreasonably change the "legal consequences of past actions" such that they undermine "reliance upon the pre-existing rule" are prohibited.[44]

As drafted, the proposed rules seek to permit the revocation of existing equipment authorizations by establishing a framework for revocations where a supplier is included on the Covered List.[45] The NPRM asks whether to the Commission should revoke existing authorizations "if the

---

[43] *See Joint Anti-Fascist Refugee Comm.* v. *McGrath*, 341 U.S. 123, 144 (1951) (Jackson, J., concurring) (stating that "officially prepared and proclaimed blacklists" inherently impose punishment and thus "possess almost every quality of [classic] bills of attainder").

[44] *Bowen* v. *Georgetown Univ. Hosp.*, 488 U.S. 204, 219-20 (1988) (Scalia, J., concurring); *see U.S. AirWaves, Inc.* v. *FCC*, 232 F.3d 227, 233 (D.C. Cir. 2000) ("A secondarily retroactive rule is valid only to the extent that it is reasonable.").

[45] NPRM, ¶¶ 82-89. Besides revoking already-effective authorizations that were obtained based on the rules then in effect (*i.e.*, prior to the effective date of any new rules in this proceeding), the NPRM proposes a revocation framework that may permit the Commission to revoke "authorizations that may have been granted under false statements or representations (including non-disclosure) concerning whether, an equipment authorization application that was subsequently granted had in fact included 'covered' equipment (in whole or as a component part)." NPRM, ¶ 83. If the proposed rules were valid – which they are not – and are adopted as a result of this proceeding, revoking authorizations, on a prospective basis, that were obtained in violation of the new rules would not be unreasonable retroactivity. Dahua agrees that the Commission has authority to revoke an authorization that was issued in violation of rules that were in effect *at the time* of the issuance.

Commission would not have granted an application with equipment from an entity on the Covered List under newly adopted rules"[46] and proposes to treat the new vendor-based prohibition as a "change to the Commission's technical standards" warranting withdrawal of existing authorizations.[47]

These proposals would permit revocation of existing equipment authorizations based on non-technical criteria and qualifications that did not exist at the time the authorizations were granted. Companies (including downstream distributors, integrators, and end-users) have made substantial investments in reliance on the ability for equipment to become authorized through the processes established by the Commission. Subject only to the limited exception required by the Anti-Drug Abuse Act of 1988, there currently is no prohibition against obtaining equipment authorization based solely on the identity of the manufacturer, including the manufacturer of any component parts of equipment for which authorization is sought. That is, market participants have acted in good faith reliance upon the Commission's rules regarding equipment authorizations, and there is no evidence that any named vendor (including Dahua) has violated any of the existing criteria or rules governing equipment authorizations. If adopted, the proposed rule therefore would have the legal effect of prohibiting the importation, marketing, sale, distribution, and use of products that were duly authorized following established processes.

Due process. Third, existing equipment authorizations are property rights that, once granted, are protected by the U.S. Constitution.[48] An individual or entity has a protectable property

---

46 NPRM, ¶ 85.

47 NRPM, ¶ 86.

48 *See, e.g.*, *Spinelli v. New York*, No. 07-1237-cv, 2009 WL 2413929 (2d Cir. Aug. 7, 2009) (holding that a business license, once granted, is a protected property interest warranting due process protection).

interest in a business license or permit where it has "more than a unilateral expectation" in the license's continued effect.[49] Where, as here, the discretion held by the government to revoke a license is limited, the licensee holds a protected property interest.

Section 2.939(a) of the Commission's rules limits the Commission's ability to revoke any equipment authorization to four circumstances: (1) false statements or representations; (2) a determination that the equipment does not conform to the pertinent technical requirements or to the representations made in the original application; (3) if changes have been made in the equipment other than those authorized by the rules or otherwise expressly authorized; and (4) conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.[50] Moreover, Section 2.939(b) requires all revocations of equipment authorizations to be conducted, if at all, in the same manner as revocation for radio station licenses (*i.e.*, only following notice to the affected party with an opportunity for a hearing during which "both the burden of proceeding with the introduction of evidence and the burden of proof shall be on the Commission"[51]).[52]

Although Section 2.939(c) permits the withdrawal of an equipment authorization "in the event of changes in [the Commission's] technical standards[,]" the identity of the manufacturer of the equipment (or component parts thereto) is not a "technical standard". Moreover, all withdrawals under that provision must be subject to procedures developed after an "appropriate rulemaking

---

49 *See 3883 Conn. LLC v. Dist. of Columbia*, 336 F.3d 1068, 1072 (D.C. Cir. 2003).

50 *See* 47 C.F.R. 2.939(a)(1)-(4).

51 47 U.S.C. § 312(d). *See also* 47 C.F.R. 1.91 (requiring issuance of an order directing the licensee or permittee to show cause why an order of revocation should not be issued and designated for a hearing).

52 *See* 47 C.F.R. 2.939(b).

proceeding" and must "provide a suitable amortization period for equipment in hands of users and in the manufacturing process."[53]

V. THE COSTS OF THE PROPOSED RULE AS APPLIED TO DAHUA OUTWEIGH ANY SPECULATIVE BENEFITS.

Beyond its legal flaws described above, proposed rules would not be a cost-effective means to prevent Covered List equipment (including equipment produced or provided by Dahua) from introduction into the U.S. market. Dahua's equipment is widely used in the U.S. marketplace. If the proposed rules are adopted, millions of Dahua devices may need to be replaced.[54] This embedded base of equipment already deployed throughout the United States (by large and small users in a wide cross-section of industry sectors) will make exorbitantly costly any effort to remove Dahua equipment from the United States. Without the ability to repair, replace or purchase new equipment, existing users in the U.S. will face significant difficulty and increased costs (including for potentially required removal and replacement of equipment already in use), and the potential for security vulnerabilities to arise if equipment cannot be timely updated or maintained.

In addition, the vast majority of Dahua's equipment is not relevant to the Commission's concerns regarding national security risks to communications networks. For example, a significant amount of Dahua equipment imported, marketed, sold, and used in the United States is used in a closed network environment entirely disconnected from the broader public network such that prohibiting Dahua's equipment would not generate any increased security benefits to communications networks.

---

53 *See* 47 C.F.R. 2.939(c).

54 Not all products sold in the U.S. by Dahua USA or its partners are devices that require equipment authorization nor are all Dahua products considered "Covered List" equipment. Dahua USA's sales include accessories such as cables, SD cards, tripods, and a variety of other non-electronic products.

Moreover, by banning equipment made by two of the leading Chinese manufacturers in the video security segment, the proposed rules will limit the supply of such equipment and therefore necessarily drive up the price paid by U.S. end-users (regardless of whether such users purchase equipment that is branded by a Covered List vendor or white-labelled and sold by another supplier). Limiting Dahua USA's access to the U.S. market would result in less competition in the U.S. security industry and higher prices for security products ultimately paid by end-users.

In addition to the costly impacts of implementing (and lack of tangible benefits derived from) the proposed rules, enforcement of the proposed rules would be extremely expensive at best and impractical at worst. If the rules are not effectively enforced, then the anticipated benefits will not be realized; but any effort to enforce them comprehensively would entail unreasonable expense. Enforcement would be extremely difficult because neither Dahua nor a TCB (nor the Commission) can determine, in advance, whether end-users will use a particular type of equipment for the specific purposes identified on the Covered List (*i.e.*, for "public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes"). Moreover, the prevalence of white-label products in the video security industry will compound the difficulty of identifying relevant products and preventing prohibited uses by end-users.

Unlike telecommunications network equipment, which is generally purchased and used by entities the Commission already regulates (and, as demonstrated by the Secure Networks Act, can gather information regarding the extent of current use of such equipment), video security equipment is widely used by a broad spectrum of private property owners, the vast majority of whom have no existing relationship with the Commission. The Commission as a result lacks any visibility

or connection to end-user customers. Nor does the Commission have any connection with distributors that acquire already-authorized equipment for resale, further compounding potential oversight and enforcement challenges.

Even assuming that the proposed rules could be enforced, they are unlikely to result in significant benefits that justify their costs. Prohibiting two specific Chinese manufacturers from obtaining equipment authorization for video security products will not eliminate the demand for such products from U.S. end users. Rather than cutting off suppliers of concern from the market, the proposed rules will only create an incentive for other suppliers, including other Chinese companies, to enter the market to meet this demand. The Commission will have to monitor this market segment, which is not part of its core responsibility or expertise, constantly to identify new suppliers whose products could potentially pose a threat to national security.

VI. CONCLUSION

For the foregoing reasons, the Commission should not adopt its proposed rules. Doing so would be unlawful, arbitrary and capricious, and would impose substantial costs that outweigh any speculative benefits. If the Commission proceeds to adopt the proposed rules (which it should not), it must make clear that the rules applies only to Dahua equipment used for the specifically delineated uses outlined in Section 889 and reflected in the Covered List.

Respectfully submitted,

/s/Andrew D. Lipman

Andrew D. Lipman
Russell M. Blau
Patricia Cave

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
patricia.cave@morganlewis.com

Counsel to Dahua Technology USA Inc.

September 20, 2021